Steganographic Data Hiding in QR Codes

Shilpa Jagtap[1*], J L Mudegaonkar[2]

[1] Department of Electronics & Telecommunication, D Y Patil College of engineering, Pune, India.
[2] Karmayogi Engineering College, Shelve, Pandharpur Dist Solapur., India

*Corresponding author

doi: https://doi.org/10.21467/proceedings.118.38

ABSTRACT

In the era of technological development, data transfer over internet is playing vital role in communication. Now a days use of internet became common and it is necessary to secure the transmission of data in the form of protecting information systems from unauthorized access, use, disruption, modification, recording or destruction. There various methods available for data security, like cryptography and steganography. Steganography is the technique in which data gets hide behind any other information and it becomes difficult for unauthorized user to detect it. QR code is the trademark for a type of matrix barcode consisting of the black square modules arranged in a square grid on a white background. Any imaging devices such as camera, scanner are used for reading the code. In this article we are discussing different technologies that can be used for steganography along with steganography using QR codes.

Keywords: Steganography, Data Hiding, QR codes, Cryptography

1 Introduction

In the world of Internet and global business, transfer of data or information has become easier. Due to ease of operation, high speed of transmission, digital communication became more popular. It became necessary to protect the data from unauthenticated access. This can be done using cryptography as well as steganography. Cryptography encrypts the data and can be detected correctly by the authenticated system and not the other. But it only Encrypts the message, and do not hide it. Instead, if we use steganography then data will get hide behind any other information and it will become difficult for unauthorized user to detect it.

Steganography means hiding information in other information. Steganography word is originated from the following Greek words "STEGOS" means 'cover' and another word "GRAFIA" means 'writing' which defines it as 'covered writing'. Other than valid user, viewing this message will fail to know it contains hidden/encrypted data. Digital steganography can be done with image, text, video and audio. Different techniques such as statistical, Machine learning, Deep learning methods have been developed for image steganography [1]. Most of the times intellectual property (IP) core may lead to piracy. We can use crypto-based steganography for providing security to IP cores, which may suffer from false claim of ownership. With stego-mark embedding in design and detecting the same, the ownership can be awarded to the genuine IP owner [2].

QR Codes are quickly readable codes through any imaging device such as camera, scanner. Even now a day we use our mobile phones for scanning the QR code. QR codes are formed of a Matrix Barcode, usually a 2-D Barcode which is a combination of spacing. When a QR Code is scanned, it passes wide multitude of information. QR Codes are having applications in industries such as retail, marketing, and logistics. Image steganographic method by embedding encoded secret message with QR code into image data can be developed using DWT and AES cipher algorithm [3]. Another method of data hiding using QR codes can be generated such that it carries its ordinary message in addition to the payload. The message can be read

Proceedings DOI: 10.21467/proceedings.118; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-6-4

by anyone and will be treated as normal QR code, but the payload can only be obtained using a secret key. The message and the payload can be developed such that both are unrelated to each other [4].

Apart from QR code technique there are different methods are developed for embedding data into images. Few techniques out them are RDH (Reversible Data Hiding), in which both images and data are covered by using mathematical methods like Difference Expansion (DE) or Histogram Shifting. Another technique is Image Steganography and Image Watermarking. In image Steganography, DCT, Edge Adaptive and DFT are the popular techniques. Watermark is a type of signature and watermarking is a process of embedding a watermark in a multimedia object. For watermarking DCT can be used [5].

Apart from QR code based steganography another approach is color image steganography for image communication over wireless communication systems. In this approach a three color image gets hide in one color cover image to increase the capacity of hiding. Cover image is transformed to chrominance and luminance and components to embed the images which is to be hidden. The chaotic Baker map can be used for secret images encryption. This will help in tolerating the channel degradations in better way. The Orthogonal Frequency Division Multiplexing system with channel equalization is used for wireless communication [6].

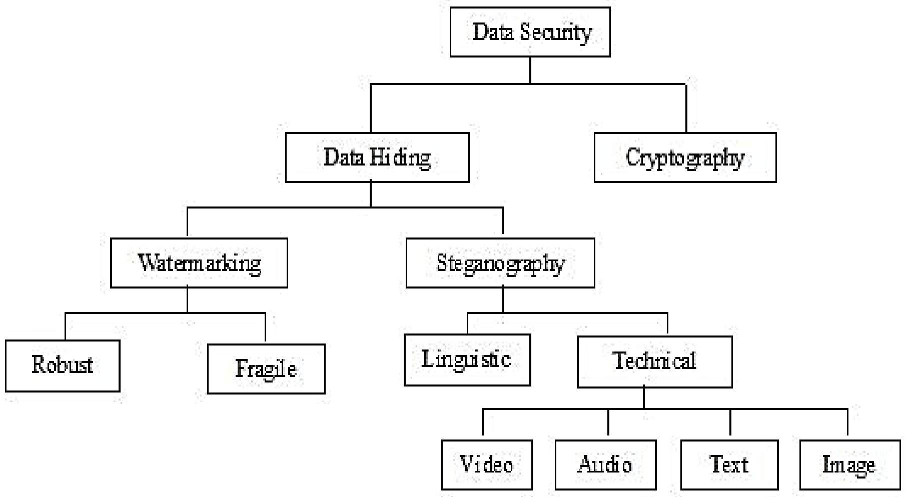

Figure 1: *Classification of Data security systems [7]*

Figure 1 shows different techniques used for securing the data. It is broadly classified into cryptography and data information hiding. In which steganography and watermarking techniques are further classified.

2 System Overview

The overview of the Steganographic Data Hiding in QR codes system is shown in figure 2. In this system the secrete data which is to be send is get encrypted by using QR codes. A unique QR code is generated for the specific data. This QR code get hide inside a colour image. Quantized QR code technique is used for data hiding. Which will not make any visible distortion in the cover image. It provides two levels of security to the information being transmitted as shown in figure. The encryption of secret message is done by using QR code generator. The QR code consists of Matrix of Black and White Pixels forms a QR code and it is difficult to read by human beings. With use of smart phone, the message hidden inside QR codes can be scanned. To avoid this colour images are used to hide the QR code. Because of this the unauthorized entities cannot easily break the system and read the message. By applying this technique, a two level of security gets achieved for the secret message transfer.

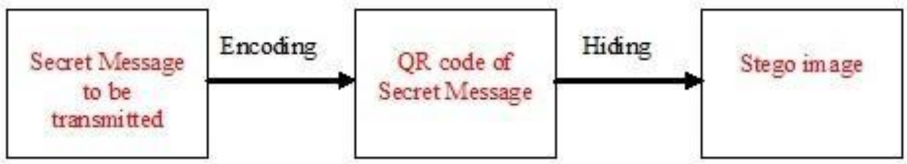

Figure 2 : *Generation of Stego image[8]*

There are different technologies that can be used in encrypting the payload. By embedding this payload with QR code improves performance of steganography.

3 Performance parameters for System analysis

Once we have developed any system, we have to analysis the system performance based on which we can decide whether the system is useful for application or not. This section gives information about some performance parameters that can be used for validation of system.

Mean Square Error (MSE)

The MSE represents the average of the squares of the "errors" between actual image and image generated after steganography [8][17]. The error is gives values of difference between the original image and degraded image.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^{2}$$

Where

f is the matrix data of original image.

g represents the matrix data of steganographic image.

m gives the numbers of rows of pixels of the images and i gives the index of that row.

n gives the number of columns of pixels of the image and j gives the index of that column.

Peak Signal to Noise Ratio (PSNR)

Peak signal-to-noise ratio can be defined as the ratio of the maximum possible power of an image to the power of noise which degrades the quality of image representation. For PSNR estimation of an image we have to compare the received image with an ideal clean image of maximum possible power. The PSNR in decibels is computed between the cover image and the steganographic image. This ratio is used as a quality measurement between the original and the steganographic image. The higher the PSNR, lesser is the difference between the cover image and the steganographic image.

$$PSNR = 10\log_{10}\left(\frac{MAXf^{2}}{MSE}\right)$$

Where

MAXf gives maximum signal value in the cover image.

The calculation of PSNR and MSE is done after hiding the QR codes are generated with secret messages of different sizes with in the same image.

Structural Similarity Index (SSIM)

It is another tool that can be used to measure the similarities between the original image and the stego-image. The range for it is in between −1 and 1 where 1 means that both images are identical . It is expressed as

$$SSIM = \frac{(2m_o m_s + c_1)(2\sigma_{os} + c_2)}{(m_o^2\, m_s^2 + c_1\,)(\sigma_o^2 + \sigma_s^2 + c_2\,)}$$

Where

m_0 is mean, m_s is variance and σ is the standard deviation of the image. The subscripts o, s represents the original and stego-images respectively. σos is the covariance between both images. Also, c1, c2 are constant having value as c1 = k1L and c2 = k2L receptively where k1 = 0.01 and k2 = 0.03 and L = 255 is the maximum value of the gray scale image.

The parameter SSIM calculation is based on visible structures in the image.

4 Conclusion

Image steganography is the secret embedding of message into digital images. It helps in protection of confidential information. QR codes on the other hand are used to encrypt the data or information, which can be obtained by scanning device such as scanner, camera or mobile phone. Both Steganography and QR codes are used for storing and transmission of data without getting damaged. When we combines these two technologies the transfer of secrete data will become easy. For encrypting payload various methods and algorithms such as DWT, ASE, RSA can be used. QR code and perfectly embedded payload leads to secure data transmission. Now a days different technologies such as Machine learning or Deep learning can explore new data hiding techniques.

References

[1] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[2] A. Sengupta and M. Rathor, "Crypto-Based Dual-Phase Hardware Steganography for Securing IP cores," *IEEE Letters of the Computer Society*, vol. 2, no. 4, pp. 32-35, 1 Dec. 2019, doi: 10.1109/LOCS.2019.2942289.

[3] V. Hajduk, M. Broda, O. Kováč and D. Levický, "Image steganography with using QR code and cryptography," *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*,2016,pp.350-353, doi: 10.1109/ RADIOELEK. 2016.7477370.

[4] M. Alajmi, I. Elashry, H. S. El-Sayed and O. S. Farag Allah, "Steganography of Encrypted Messages Inside Valid QR Codes," *IEEE Access*, vol. 8, pp. 27861-27873, 2020, doi: 10.1109/ACCESS.2020.2971984.

[5] R. Zaheer, R. S. Gaur and V. Dixit, "A literature survey on various approaches of data hiding in images," *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2017, pp. 1-5, doi: 10.1109/ICIIECS.2017.8276104.

[6] Eyssa, A.A., Abdelsamie, F.E. & Abdelnaiem, A.E., "An Efficient Image Steganography Approach over Wireless Communication System," *Wireless Pers Commun* 110, 321–337 (2020). https://doi.org/10.1007/s11277-019-06730-2

[7] Inas Jawad Kadhim *et al*., "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, Volume 335,2019,Pages299-326,ISSN 0925-2312, https://doi.org/ 10.1016/ j.neucom. 2018.06.075.

[8] M. Mary Shanthi Rani and K.Rosemary Euphrasia,"Data security through QR code encryption and steganography," *Advanced Computing: An International Journal (ACIJ),* Vol.7, No.1/2, March 2016, DOI:10.5121/acij.2016.7201

[9] Wu WC., Lin ZW., Wong WT. , " Application of QR-Code Steganography Using Data Embedding Technique," *Information Technology Convergence. Lecture Notes in Electrical Engineering*, vol 253. Springer, Dordrecht., 2013 ,https://doi.org/10.1007/978-94-007-6996-0_63

[10] A. Mendhe, D. K. Gupta and K. P. Sharma, "Secure QR-Code Based Message Sharing System Using Cryptography and

Steganography," *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 188-191, doi: 10.1109/ICSCCC.2018.8703311.

[11] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826-832, April 2012, doi: 10.1109/TIFS.2011.2176120.

[12] R. Jain and J. Boaddh, "Advances in digital image steganography," *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 2016, pp. 163-171, doi: 10.1109/ICICCS.2016.7542298.

[13] S. Zhang, Z. Yang, J. Yang and Y. Huang, "Linguistic Steganography: From Symbolic Space to Semantic Space," *IEEE Signal Processing Letters,* vol. 28, pp. 11-15, 2021, doi: 10.1109/LSP.2020.3042413.

[14] X. Zhang, F. Peng and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, Dec. 2018, doi: 10.1109/TMM. 2018.2838334.

[15] P. Zhang, C. Li and C. Wang, "VisCode: Embedding Information in Visualization Images using Encoder-Decoder Network," *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 2, pp. 326-336, Feb. 2021, doi: 10.1109/TVCG.2020.3030343.

[16] P. Lin and Y. Chen, "QR code steganography with secret payload enhancement," *2016 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, 2016, pp. 1-5, doi: 10.1109/ICMEW.2016.7574744.

[17] A. S. Brandao and D. C. Jorge, "Artificial Neural Networks Applied to Image Steganography," *IEEE Latin America Transactions*, vol. 14, no. 3, pp. 1361-1366, March 2016, doi: 10.1109/TLA.2016.7459621.

[18] A. A. Lopez-Hernandez, R. F. Martinez-Gonzalez, J. A. Hernandez-Reyes, L. Palacios-Luengas and R. Vazquez-Medina, "A Steganography Method Using Neural Networks," *IEEE Latin America Transactions*, vol. 18, no. 03, pp. 495-506, March 2020, doi: 10.1109/TLA.2020.9082720.

[19] L. M. Marvel, C. T. Retter and C. G. Boncelet, "A methodology for data hiding using images," *IEEE Military Communications Conference. Proceedings. MILCOM 98* (Cat. No.98CH36201), 1998, pp. 1044-1047 vol.3, doi: 10.1109/MILCOM.1998.727007.